APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/086,302	02/28/2002	Alexander Medvinsky	018926-008400US	2065

20350	7590	10/04/2005	

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/086,302	MEDVINSKY, ALEXANDER
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *February 2, 2002*.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-26* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some * c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *10/06/03*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-26 have been examined.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

3.   Claims 12, 21 and 26 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

Claim 12 recite "a method" in the preamble, however, the independent claim 4 in

which claim 12 depend on recite "a system". Appropriate correction is required.

Claim 21 recite "a method" in the preamble, however, the independent claim 18

in which claim 21 depend on recite "a system". Appropriate correction is required.

Claim 26 recite "a method" in the preamble, however, the independent claim 18

in which claim 26 depend on recite "a system". Appropriate correction is required.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-8, 11-13 and 17-26 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Yang United States Letter Patent Number 6,069,877 in view of

Willins et al. (hereinafter Willins) United States Publication Number 2001/0052083.

As per claim 1:

Yang discloses a method for detecting clones (unauthorized duplicate identities)

of the client, the method comprising:

forwarding a first signal from a client , the first signal for requesting access to a

server; (Col. 2, lines 44-61; Col. 3, lines 39-45 and lines 59-60; Col. 10, lines 43-45)

verifying that the client is authorized to access the server; (Col. 4, lines 4-5)

receiving a second signal from an entity, the second signal for requesting access

to the server, wherein the entity has identifying information identical to the client; (Col. 4,

lines 6-9) and

if the second request is received prior to expiration of the time T, either marking

the entity as a possible clone or denying the second request in order to prevent access

to the server. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with

one or more of the plurality of client units and communicating information between a

host computer and one or more mobile communication units. (Col. 2, lines 57-61 and

Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and transmitting a ticket from the KDC to

the client, the ticket for providing access to the server, wherein the ticket is valid for a

time T.

Willins in analogous art, however, disclose a KDC and transmitting a ticket from

the KDC to the client, the ticket for providing access to the server, wherein the ticket is

valid for a time T. (Figure 13; Page 8, paragraph 93)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the system disclosed by Yang to include

transmitting a ticket from the KDC to the client, the ticket for providing access to the

server, wherein the ticket is valid for a time T. This modification would have been

obvious because a person having ordinary skill in the art would have been motivated to

do so, as suggested by, Willins (Page 2, paragraph 15) in order to provide reliable,

authorized user access to a network, especially to electronic services in a wireless

network.

As per claim 2:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Willins further discloses a method comprising providing a session key in the ticket, the

session key being valid for a designated duration. (Page 2, paragraph 18)

As per claim 3:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Willins further discloses a method wherein the designated duration is for determining

the time T for which the ticket is valid. (Page 2, paragraph 20)

As per claims 4, 13 and 18:

Yang teaches a system for detecting clones of a client within a communication

network, the system comprising:

an application server communicably; (Figure 1, Col. 3, line 39)

a client for providing a first request to access the application server; (Figure 1,

Col. 3, lines 37-38)

receiving a second request to access the application server, the second request

being received from an entity having identifying information identical to the client; (Col.

4, lines 6-9) and

if the second request is received during time T, denying the second request to

prevent the entity from accessing the application server. (Col. 4, lines 9-14; Col. 11,

lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with

one or more of the plurality of client units and communicating information between a

host computer and one or more mobile communication units. (Col. 2, lines 57-61 and

Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and responsive to the first request, the

KDC forwarding a first ticket for accessing the application server, the first ticket being

valid for a time duration T.

Willins in analogous art, however, discloses a KDC; (Figure 13; Page 8,

paragraph 91) responsive to the first request, the KDC forwarding a first ticket for

accessing the application server, the first ticket being valid for a time duration T. (Figure

13; Page 8, paragraph 93)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the system disclosed by Yang to include a

KDC and responsive to the first request, the KDC forwarding a first ticket for accessing

the application server, the first ticket being valid for a time duration T. This modification

would have been obvious because a person having ordinary skill in the art would have

been motivated to do so, as suggested by, Willins (Page 2, paragraph 15) in order to

provide reliable, authorized user access to a network, especially to electronic services in

a wireless network.

As per claim 5:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Yang further discloses a system wherein the entity is a clone. (Col. 2, line 45)

As per claims 6, 16, 24 and 25:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Yang further discloses a system wherein the identifying information is a client identifier

copied by the clone. (Col. 3, lines 1-4)

As per claim 7:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Willins further discloses a system wherein the ticket further comprises an encrypted

session key. (Page 2, paragraph 20)

As per claim 8:

Yang and Willins disclose all the subject matter as discussed above. In addition, Willins further discloses a system comprising the client deriving a copy of the session key for accessing the application server. (Page 8, paragraph 94)

As per claims 11, 12 and 20:

Yang and Willins disclose all the subject matter as discussed above. In addition, Willins further discloses a system comprising using a key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC. (Page 8, paragraphs 89-94)

As per claim 17:

Yang and Willins disclose all the subject matter as discussed above. In addition, Yang further discloses a system comprising the key management means denying access to the first computing device, if more than M requests are received. (Col. 11, lines 59-60)

As per claim 19:

Yang and Willins disclose all the subject matter as discussed above. In addition, Willins further discloses a system comprising the KDC encrypting a session key within the ticket; and the client extracting a copy of the session key in a manner that no entity other than the client can access the session key. (Page 2, paragraph 17)

As per claims 21 and 23:

Yang and Willins disclose all the subject matter as discussed above. In addition, Willins further discloses a system wherein a ticket granting server is the server, and the ticket is a ticket granting ticket. (Page 8, paragraph 91)

As per claim 22:

Yang teaches a method for detecting clones in a communication network, the method comprising:

receiving a request to access the KDC, the request being received from an entity with the same identifying information as the authorized client; (Col. 4, lines 6-9) and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access. (Col. 2, line 45; Col. 4, lines 9-14; Col. 11, lines 21-28)

In addition, Yang further discloses a base stations for establishing a session with one or more of the plurality of client units and communicating information between a host computer and one or more mobile communication units. (Col. 2, lines 57-61 and Col. 3, lines 40-45).

Yang does not explicitly disclose a KDC and providing a ticket to an authorized client, the ticket for accessing a KDC, the ticket having a session key valid for a time duration T;

Willins in analogous art, however, discloses a KDC; (Figure 13; Page 8, paragraph 91) providing a ticket to an authorized client, the ticket for accessing a KDC, the ticket having a session key valid for a time duration T. (Figure 13; Page 8, paragraph 93)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Yang to include a KDC and providing a ticket to an authorized client, the ticket for accessing a KDC, the ticket having a session key valid for a time duration T. This modification would have

been obvious because a person having ordinary skill in the art would have been

motivated to do so, as suggested by, Willins (Page 2, paragraph 15) in order to provide

reliable, authorized user access to a network, especially to electronic services in a

wireless network.

As per claim 26:

Yang and Willins disclose all the subject matter as discussed above. In addition,

Willins further discloses a system wherein the KDC is the server. (Page 8, paragraph

91)

6.   Claims 9-10 and 14-16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Yang United States Letter Patent Number 6,069,877 in view of

Willins et al. (hereinafter Willins) United States Publication Number 2001/0052083

further in view of Tung et al. Public Key Cryptography for Initial Authentication in

Kerberos, Internet Draft, (hereinafter Tung).

As per claim 9:

Yang and Willins disclose all the subject matter as discussed above. Both

references do not explicitly disclose a system wherein the session key is derived using

a key agreement algorithm.

Tung in analogous art, however, discloses a system wherein the session key is

derived using a key agreement algorithm. (Section 2, paragraph 2)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the system disclosed by Yang and Willins

to include a system wherein the session key is derived using a key agreement

algorithm. This modification would have been obvious because a person having

ordinary skill in the art would have been motivated to do so, as suggested by, Tung

(Section 2, paragraph 4) in order to enable access to Kerberos-secured services based

on initial authentication using public key cryptography.

As per claim 10:

Yang, Willins and Tung disclose all the subject matter as discussed above. In

addition, Tung further discloses a system wherein the key agreement algorithm is the

Diffie-Hellman algorithm. (Section 2, paragraph 3)

As per claim 14:

Yang and Willins disclose all the subject matter as discussed above. Both

references do not explicitly disclose a system wherein the key management means

utilizes Diffie-Hellman algorithm to distribute session keys.

Tung in analogous art, however, discloses a system wherein the key

management means utilizes Diffie-Hellman algorithm to distribute session keys.

(Section 2, paragraph 3)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the system disclosed by Yang and Willins

to include a system wherein the key management means utilizes Diffie-Hellman

algorithm to distribute session keys. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so,

as suggested by, Tung (Section 2, paragraph 4) in order to enable access to Kerberos-

secured services based on initial authentication using public key cryptography.

As per claim 15:

Yang, Willins and Tung disclose all the subject matter as discussed above. In

addition, Yang further discloses a system comprising the key management means

flagging the entity if more than M requests are received from the entity. (Col. 9, lines 59-

60)

As per claims 16:

Yang, Willins and Tung disclose all the subject matter as discussed above. In

addition, Yang further discloses a system wherein the identifying information is a client

identifier copied by the clone. (Col. 3, lines 1-4)

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. See PTO Form-892.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-

4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
09/30/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100